RECEIVED
CENTRAL FAX CENTER

SEP 13 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of: Keith A. Harrison, *et al.*	Confirmation No.: 4475
Serial No.: 09/918,326	Group Art Unit: 2137
Filed: July 30, 2001	Examiner: Schubert, Kevin R.
For: Authentication Method in a Printing Environment	HP Docket No. 30006788-2 TKHR Docket No. 050828-1020

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. § 41.37 is submitted in support of the Notice of Appeal filed June 13, 2006, responding to the Final Office Action mailed March 15, 2006 and the Advisory Action mailed June 27, 2006.

It is not believed that extensions of time or fees are required to consider this Appeal Brief. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required therefor are hereby authorized to be charged to Deposit Account No. 08-2025.

09/14/2006 MBINAS 00000055 082025 09918326
01 FC:1402 500.00 DA

RECEIVED
CENTRAL FAX CENTER

SEP 13 2006

I. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. Related Appeals and Interferences

There are no known related appeals or interferences that will affect or be affected by a decision in this Appeal.

III. Status of Claims

Claims 1-16 stand finally rejected. No claims have been allowed. The final rejections of claims 1-16 are appealed.

IV. Status of Amendments

This application was originally filed on July 30, 2001, with eleven (11) claims. In a Response filed May 9, 2005, Applicant amended claims 1 and 11 and added claims 12-16. In a Response filed September 12, 2005, Applicant amended claims 1, 10, and 11. In a Response filed February 23, 2006, Applicant amended claims 1, 10, and 11. The claims in the attached Claims Appendix reflect the present state of Applicant's claims.

V. Summary of Claimed Subject Matter

The claimed inventions are summarized below with reference numerals and references to the written description ("specification") and drawings. The subject matter described in the following appears in the original disclosure at least where indicated, and may further appear in other places within the original disclosure.

Embodiments according to independent claim 1 describe a document printout device for receiving and printing out digital documents. The printout device comprises a store of digital certificates (Figure 4, 90), each certificate (Figure 4, 18) being associated with a received digital document (Figure 4, 24) and a most recent sender of the received digital document (Figure 4, 24) which is to be printed. The device further comprises an audit log (Figure 4, 94) comprising a list of received document entries, each entry containing a reference to one of the certificates (Figure 4, 18) in the store (Figure 4, 90), an encrypted digest (Figure 4, 86) corresponding to the received digital document of that entry, and a unique identifier associated with the received digital documents. Applicant's specification, page 23, lines 14-20. A decryption algorithm is included in the device for decrypting the received encrypted digest (Figure 4, 86) associated with one of the received digital document (Figure 4, 24) selected for verification. Applicant's specification, page 18, lines 18-24. The device further includes a hash algorithm (Figure 4, 92) for creating a digest of the selected digital document such that when the created digest corresponds to the decrypted digest, the digital certificate of the most recent sender is authenticated. The received digital document (Figure 4, 24), the received encrypted digest (Figure 4, 86) associated with the received digital document, and the digital certificate (Figure 4, 18) associated with the received digital document are received contemporaneously, and the document printout device is configured to print the received digital document

(Figure 4, 24) upon the digital certificate (Figure 4, 18) of the most recent sender being authenticated. Applicant's specification, pages 22-26, lines 6-18.

Embodiments according to independent claim 10 describe a device in a facsimile machine adapted for receiving and printing out digital documents. The device comprises a store of digital certificates (Figure 4, 90), each certificate (Figure 4, 18) being associated with a most recent sender of a received digital document (Figure 4, 24). The device further comprises an audit log (Figure 4, 94) comprising a list of received document entries, each entry containing a reference to one of the certificates in the store and a unique identifier associated with a received digital document (Figure 4, 24). Applicant's specification, page 23, lines 14-20. The received digital document (Figure 4, 24) and a digital certificate (Figure 4, 18) of a most recent sender of the received digital document are received contemporaneously by the facsimile machine (Figure 4, 74). The facsimile machine (Figure 4, 74) is configured to print the received digital document (Figure 4, 24) upon the most recent sender of the received digital document being authenticated. Applicant's specification, pages 22-26, lines 6-18.

Embodiments according to independent claim 11 describe a method of authenticating the identity of a sender of a received digital document. The method comprises using a unique identifier printed on the received document (Figure 4, 24) to search for a corresponding record in a list of received document records. Applicant's specification, page 23, lines 14-20 and step 136 of Figure 6. The method further comprises referencing a digital certificate (Figure 4, 18) associated with the selected record, the certificate being one of a store of certificates (Figure 4, 90) of received documents and each digital certificate (Figure 4, 18) being associated with a most recent sender of a received digital document (Figure 4, 24). Applicant's specification,

page 24, lines 3-12 and steps 110-112 of Figure 5. Such a method further comprises receiving an encrypted digest of the received digital document (Figure 4, 86) and decrypting the encrypted digest (Figure 4, 86). Applicant's specification, page 24, lines 13-21 and steps 122-124 of Figure 6. The method further comprises computing a value of a second digest from the received digital document (Figure 4, 24) and comparing the computed value of the second digest with a value of the decrypted digest. Applicant's specification, page 24, lines 13-25 and steps 126-128 of Figure 6. Such a method further comprises carrying out an on-line authentication of the certificate when the computed value of the second digest corresponds with the value of the decrypted digest and printing the received digital document (Figure 4, 24) if the certificate (Figure 4, 18) of the most recent sender of the received digital document is authenticated, wherein the received digital document (Figure 4, 24), the received encrypted digest (Figure 4, 86) associated with the received digital document, and the digital certificate (Figure 4, 18) associated with the received digital document are received contemporaneously. Applicant's specification, pages 24-25, lines 26-8 and steps 132-140 of Figure 6.

VI. Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejections are to be reviewed on appeal:

Claim 10 has been rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by *Mazzagatte* (U.S. Patent No. 6,862,583).

Claims 1-4, 9, and 11-16 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Mazzagatte* in view of *Slick* (U.S. Patent No. 7,003,667).

Claims 5-7 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Mazzagatte* in view of *Slick* in further view of *Fischer* (EP Patent 0386867B1).

Claim 8 stands rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Mazzagatte* in view of *Slick* in further view of *Mandelbaum* (EP Patent No. 0671830A2).

VII. Arguments

The Appellant respectfully submits that Applicant's claim 10 is patentable under 35 U.S.C. § 102 and claims 1-9 and 11-16 are patentable under 35 U.S.C. § 103. The Appellant respectfully requests that the Board of Patent Appeals overturn the final rejection of those claims at least for the reasons discussed below.

A. Claim Rejections - 35 U.S.C. § 102(e)

Claim 10 has been rejected under 35 U.S.C. § 102(e) as being anticipated by *Mazzagatte* (U.S. Patent No. 6,862,583). Applicant respectfully traverses this rejection.

It is axiomatic that "[a]nticipation requires the disclosure in a single prior art reference of each element of the claim under consideration." *W. L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554, 220 USPQ 303, 313 (Fed. Cir. 1983). Therefore, every claimed feature of the claimed invention must be represented in the applied reference to constitute a proper rejection under 35 U.S.C. § 102(e).

In the present case, not every feature of the claimed invention is represented in the *Mazzagatte* reference. Applicant discusses the *Mazzagatte* disclosure and Applicant's claims in the following.

1. The *Mazzagatte* Disclosure

Mazzagatte describes a system and method for authenticated secure printing. In Mazzagatte's method, a sender submits a print job along with a unique identification information that *identifies the person who is the intended recipient* of the job. Col. 8, lines 19-22. The print job is then received by a "print node," which can comprise a printer or a gateway (*e.g.*, server) to one or more printers. Col. 7, lines 39-41; col. 8, lines 62-63. Upon receiving the data, the print node processes the print data (*e.g.*, encrypts the print data) and waits for the intended recipient to arrive at the printer and present proper authentication information in order to retrieve the print job and have it printed. Col. 9, lines 8-10; lines 32-35.

2. Claim 10

Mazzagatte fails to teach several of Applicant's claim limitations. Applicant discusses some of those claim limitations in the following.

Applicant's independent claim 10 provides as follows (emphasis added):

> In a facsimile machine adapted for receiving and printing out digital documents, a device comprising:
> a store of digital certificates, each certificate being associated with a most recent sender of a received digital document; and
> an audit log comprising a list of received document entries, each entry containing a reference to one of the certificates in the store and a unique identifier associated with a received digital document, ***wherein:***
> the received digital document and a digital certificate of a most recent sender of the received digital document are received contemporaneously by the facsimile machine; and
> ***the facsimile machine is configured to print the received digital document upon the most recent sender of the received digital document being authenticated.***

Applicants respectfully submit that independent claim 10 is allowable for at least the reason that *Mazzagatte* does not disclose, teach, or suggest at least that "the facsimile machine is configured to print the received digital document upon the most

recent sender of the received digital document being authenticated," as recited and emphasized above in claim 10.

In making the rejection, the final Office Action mailed March 15, 2006 stated that "Mazzagatte teaches a method of authenticated secure printing in which a print node . . . waits for an intended recipient to arrive at the printer and present proper authentication. Once the intended recipient is authenticated, the printer then determines whether there are any print jobs queued for the intended recipient, and the print node may accordingly print a document." Final Office Action, page 3.

Assuming arguendo that *Mazzagatte* teaches the foregoing, *Mazzagatte* expressly states that the "print node then waits for the intended recipient to arrive at the printer and present the proper authentication information in order to retrieve the print job and have it printed." Col. 9, lines 31-35. However, in contrast, the claim recites that a "facsimile machine is configured to print the received digital document upon the most recent sender of the received digital document being authenticated," as opposed to the intended recipient. Therefore, *Mazzagatte* does not teach or suggest all of the claimed features.

For at least this reason, claim 10 is not anticipated by *Mazzagatte*, and the claim should be allowed.

Regarding the Advisory Action mailed June 27, 2006, it iterates that "Mazzagatte teaches that the intended recipient and the most recent sender may be one and the same (Col 7, lines 11-20)." In particular, *Mazzagatte* states that "the term 'sender/intended recipient' refers to the person holding the proper authentication information to retrieve the image from the image forming device." Col. 7, lines 24-27. As such, even if an individual sends a message, his or her authentication is not checked or authenticated as to whether the individual sent an image to an image

forming device. Rather, authentication is checked at the retrieval of the printout. Therefore, in *Mazzagatte*, this same individual may attempt to receive the image at the image forming device and his or her authentication is then checked at that time (as a recipient) to determine whether the individual is the intended recipient of the image. For example, *Mazzagatte* states that "[i]n some cases, the sender and the intended recipient may be one in the same. That is, the person who sends the print job may intend that he/she be the only person to retrieve the printout from the image forming device." Col. 7, lines 17-21 (Emphasis added).

Therefore, Applicant respectfully submits that *Mazzagatte* fails to teach or suggest at least a "facsimile machine is configured to print the received digital document upon the most recent sender of the received digital document being authenticated," as recited in claim 10. For at least these reasons, the rejection should be withdrawn, and claim 10 should be allowed.

3. Summary

Due to the shortcomings of the *Mazzagatte* reference described in the foregoing, Applicant respectfully asserts that *Mazzagatte* does not anticipate Applicant's claim. Therefore, Applicant respectfully requests that the rejection of the claim be withdrawn.

B. Claim Rejections - 35 U.S.C. § 103(a)

Claims 1-4, 9, and 11-16 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Mazzagatte* in view of *Slick* (U.S. Patent No. 7,003,667). Claims 5-7 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Mazzagatte* in view of *Slick* in further view of *Fischer* (EP Patent 0386867B1). Claim 8 stands rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over

Mazzagatte in view of *Slick* in further view of *Mandelbaum* (EP Patent No. 0671830A2). It is well-established at law that, for a proper rejection of a claim under 35 U.S.C. § 103 as being obvious based upon a combination of references, the cited combination of references must disclose, teach, or suggest, either implicitly or explicitly, all elements/features/steps of the claim at issue. *See, e.g., In Re Dow Chemical*, 5 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1988), and *In re Keller*, 208 U.S.P.Q.2d 871, 881 (C.C.P.A. 1981). Applicant respectfully traverses this rejection.

1. The *Mazzagatte* Disclosure

Mazzagatte describes a system and method for authenticated secure printing. In Mazzagatte's method, a sender submits a print job along with a unique identification information that *identifies the person who is the intended recipient* of the job. Col. 8, lines 19-22. The print job is then received by a "print node," which can comprise a printer or a gateway (*e.g.*, server) to one or more printers. Col. 7, lines 39-41; col. 8, lines 62-63. Upon receiving the data, the print node processes the print data (*e.g.*, encrypts the print data) and waits for the intended recipient to arrive at the printer and present proper authentication information in order to retrieve the print job and have it printed. Col. 9, lines 8-10; lines 32-35.

2. The *Slick* Disclosure

Slick discloses a system and method "arrangement whereby a printed or faxed document can only be generated at an intended image output device in the presence of an intended recipient." Col. 1, lines 35-38.

In one embodiment, *Slick* discloses:

> In step S908, the intended recipient arrives at the location of the intended printer and inserts a smart-card belonging to the intended

recipient into a smart-card interface device which is connected to the intended printer. Preferably, the smart-card contains a unique private key and also contains authenticating identification information corresponding to the intended recipient. The printer, via the smart-card interface device, obtains the authenticating identification information of the intended recipient from the smart-card and determined whether the identification of the intended recipient is authentic (step S909). If the identification information is not authentic, control passes to the end in step S919. If the identification information is authentic, the print queue, which is located in either the printer itself or in a local server, is queried, preferably by reference to the identification of the intended recipient, to determine if there are any print jobs corresponding to the intended recipient (step S910). If there are not any print jobs in the print queue corresponding to the intended recipient, control passes to the end in step S919. If, on the other hand, there is a print job in the print queue corresponding to the intended recipient, the next sequential print job in the print queue is obtained and control passes to step S911.

. . .

If, however, the integrity of the decrypted data is verified in step S916, control passes to step S918 in which an image is printed by the intended printer in accordance with the decrypted data (step S912). Control then passes to the end in step S919.

Cols. 16-18, lines 57-20.

3. Claims 1-4 and 9

Applicant's independent claim 1 provides as follows (emphasis added):

A document printout device for receiving and printing out digital documents, the printout device comprising:

a store of digital certificates, each certificate being associated with a received digital document and a most recent sender of the received digital document;

an audit log comprising a list of received document entries, each entry containing a reference to one of the certificates in the store, an encrypted digest corresponding to the received digital document of that entry, and a unique identifier associated with the received digital documents;

a decryption algorithm for decrypting the received encrypted digest associated with one of the received digital document selected for verification; and

a hash algorithm for creating a digest of the selected digital document such that when the created digest corresponds to the

> decrypted digest, the digital certificate of the most recent sender is authenticated, wherein:
>
> the received digital document, the received encrypted digest associated with the received digital document, and the digital certificate associated with the received digital document are received contemporaneously by the document printout device; and
>
> ***the document printout device is configured to print the received digital document upon the digital certificate of the most recent sender being authenticated.***

Applicants respectfully submit that independent claim 1 is allowable for at least the reason that *Mazzagatte* in view of *Slick* does not disclose, teach, or suggest at least that "the document printout device is configured to print the received digital document upon the digital certificate of the most recent sender being authenticated," as recited and emphasized above in claim 1.

For example, *Mazzagatte* states that the "print node then waits for the intended recipient to arrive at the printer and present the proper authentication information in order to retrieve the print job and have it printed." Col. 9, lines 31-35. However, in contrast, the claim recites that "the document printout device is configured to print the received digital document upon the digital certificate of the most recent sender being authenticated," as opposed to the intended recipient. (Emphasis added).

Slick is legally inadequate to cure the deficiencies of the *Mazzagatte*, and therefore, a *prima facie* case establishing an obviousness rejection by *Mazzagatte* in view of *Slick* has not been made. Accordingly, claim 1 and claims 2-4 and 9 (which depend therefrom) are not obvious under the proposed combination of *Mazzagatte* in view of *Slick*, and the rejections should be withdrawn.

Regarding the Advisory Action mailed June 27, 2006, it iterates that "Mazzagatte teaches that the intended recipient and the most recent sender may be one and the same (Col 7, lines 11-20)." In particular, *Mazzagatte* states that "the term 'sender/intended recipient' refers to the person holding the proper authentication

information to retrieve the image from the image forming device." Col. 7, lines 24-27. As such, even if an individual sends a message, his or her authentication is not checked or authenticated as to whether the individual sent an image to an image forming device. Rather, authentication is checked at the retrieval of the printout. Therefore, in *Mazzagatte*, this same individual may attempt to receive the image at the image forming device and his or her authentication is then checked at that time (as a recipient) to determine whether the individual is the intended recipient of the image. In particular, *Mazzagatte* states that "[i]n some cases, the sender and the intended recipient may be one in the same. That is, the person who sends the print job may intend that he/she be the only person to retrieve the printout from the image forming device." Col. 7, lines 17-21 (Emphasis added). Therefore, Applicant respectfully submits that *Mazzagatte* fails to teach or suggest at least wherein "the document printout device is configured to print the received digital document upon the digital certificate of the most recent sender being authenticated," as recited in claim 1.

Likewise, *Slick* states that "a printed or faxed document can only be generated at an intended image output device in the presence of an intended recipient." Col. 1, lines 35-38. Therefore, the proposed combination of *Mazzagatte* in view of *Slick* fails to teach or suggest all of the features of claim 1 and claims 2-4 and 9 which depend therefrom.

For at least these reasons, the rejections should be withdrawn, and claims 1-4 and 9 should be allowed.

4. Claims 5-7

All of the claimed features of independent claim 1 are not taught and suggested by *Mazzagatte* and *Slick*, as previously discussed. Further, the cited art of *Fischer* fails to cure the deficiencies of the *Mazzagatte* and *Slick* references in suggesting or teaching all of the claimed features in claims 5-7. Therefore, a *prima facie* case establishing an obviousness rejection by the proposed combination of *Mazzagatte* in view of *Slick* in further view of *Fischer* has not been made. Therefore, the rejections of claims 5-7 should be withdrawn.

5. Claim 8

All of the claimed features of independent claim 1 are not taught and suggested by *Mazzagatte* and *Slick*, as previously discussed. Further, the cited art of *Mandelbaum* fails to cure the deficiencies of the *Mazzagatte* and *Slick* references in suggesting or teaching all of the claimed features in claim 8. Therefore, a *prima facie* case establishing an obviousness rejection by the proposed combination of *Mazzagatte* in view of *Slick* in further view of *Mandelbaum* has not been made. Therefore, the rejection of claim 8 should be withdrawn.

6. Claims 11-16

Applicant's independent claim 11 provides as follows (emphasis added):

> A method of authenticating the identity of a sender of a received digital document, the method comprising:
> using a unique identifier printed on the received document to search for a corresponding record in a list of received document records;
> referencing a digital certificate associated with the selected record, the certificate being one of a store of certificates of received documents and each digital certificate being associated with a most recent sender of a received digital document;

receiving an encrypted digest of the received digital document;

decrypting the encrypted digest;

computing a value of a second digest from the received digital document;

comparing the computed value of the second digest with a value of the decrypted digest;

carrying out an on-line authentication of the certificate when the computed value of the second digest corresponds with the value of the decrypted digest;

printing the received digital document if the certificate of the most recent sender of the received digital document is authenticated, wherein the received digital document, the received encrypted digest associated with the received digital document, and the digital certificate associated with the received digital document are received contemporaneously.

Applicants respectfully submit that independent claim 11 is allowable for at least the reason that *Mazzagatte* in view of *Slick* does not disclose, teach, or suggest at least "printing the received digital document if the certificate of the most recent sender of the received digital document is authenticated, wherein the received digital document, the received encrypted digest associated with the received digital document, and the digital certificate associated with the received digital document are received contemporaneously," as recited and emphasized above in claim 11.

For example, *Mazzagatte* states that the "print node then waits for the intended recipient to arrive at the printer and present the proper authentication information in order to retrieve the print job and have it printed." Col. 9, lines 31-35 (Emphasis added). However, in contrast, the claim recites that "printing the received digital document if the certificate of the most recent sender of the received digital document is authenticated, wherein the received digital document, the received encrypted digest associated with the received digital document, and the digital certificate associated with the received digital document are received contemporaneously." (Emphasis added). Therefore, *Mazzagatte* does not teach or suggest at least the above-recited feature.

Further, *Slick* is legally inadequate to cure the deficiencies of the *Mazzagatte*, and therefore, a *prima facie* case establishing an obviousness rejection by *Mazzagatte* in view of *Slick* has not been made. Accordingly, claim 11 and claims 12-16 (which depend therefrom) are not obvious under the proposed combination of *Mazzagatte* in view of *Slick*, and the rejections should be withdrawn.

Regarding the Advisory Action mailed June 27, 2006, it iterates that "Mazzagatte teaches that the intended recipient and the most recent sender may be one and the same (Col 7, lines 11-20)." In particular, *Mazzagatte* states that "the term 'sender/intended recipient' refers to the person holding the proper authentication information to retrieve the image from the image forming device." Col. 7, lines 24-27. As such, even if an individual sends a message, his or her authentication is not checked or authenticated as to whether the individual sent an image to an image forming device. Rather, authentication is checked at the retrieval of the printout. Therefore, in *Mazzagatte*, this same individual may attempt to receive the image at the image forming device and his or her authentication is then checked at that time (as a recipient) to determine whether the individual is the intended recipient of the image. For example, *Mazzagatte* states that "[i]n some cases, the sender and the intended recipient may be one in the same. That is, the person who sends the print job may intend that he/she be the only person to retrieve the printout from the image forming device." Col. 7, lines 17-21 (Emphasis added).

Therefore, Applicant respectfully submits that *Mazzagatte* fails to teach or suggest at least "printing the received digital document if the certificate of the most recent sender of the received digital document is authenticated, wherein the received digital document, the received encrypted digest associated with the received digital

document, and the digital certificate associated with the received digital document are received contemporaneously," as recited in claim 11.

Likewise, *Slick* states that "a printed or faxed document can only be generated at an intended image output device in the presence of an intended recipient." Col. 1, lines 35-38. Therefore, the proposed combination of *Mazzagatte* in view of *Slick* fails to teach or suggest all of the features of claim 11 and claims 12-16 which depend therefrom. For at least these reasons, the rejections should be withdrawn, and claims 11-16 should be allowed.

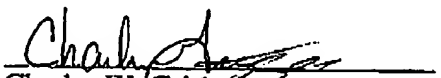
7. Summary

Due to the shortcomings of the *Mazzagatte* reference, *Slick* reference, and the other cited references described in the foregoing, Applicant respectfully asserts that Applicant's claims are patentable over the cited art. Therefore, Applicant respectfully requests that the rejection of the claim be withdrawn.

VIII. Conclusion

In summary, it is Applicant's position that Applicant's claims are patentable over the applied cited art references and that the rejection of these claims should be withdrawn. Appellant therefore respectfully requests that the Board of Appeals overturn the Examiner's rejection and allow Applicant's pending claims.

Respectfully submitted,

By: 
Charles W. Griggers
Registration No. 47,283

Claims Appendix under 37 C.F.R. § 41.37(c)(1)(viii)

The following are the claims that are involved in this Appeal.

1. A document printout device for receiving and printing out digital documents, the printout device comprising:

a store of digital certificates, each certificate being associated with a received digital document and a most recent sender of the received digital document which is to be printed;

an audit log comprising a list of received document entries, each entry containing a reference to one of the certificates in the store, an encrypted digest corresponding to the received digital document of that entry, and a unique identifier associated with the received digital documents;

a decryption algorithm for decrypting the received encrypted digest associated with one of the received digital document selected for verification; and

a hash algorithm for creating a digest of the selected digital document such that when the created digest corresponds to the decrypted digest, the digital certificate of the most recent sender is authenticated, wherein:

the received digital document, the received encrypted digest associated with the received digital document, and the digital certificate associated with the received digital document are received contemporaneously; and

the document printout device is configured to print the received digital document upon the digital certificate of the most recent sender being authenticated.

2. A device according to Claim 1, wherein the device is arranged to carry out an on-line authentication of a received certificate held in the store of received documents.

3. A device according to Claim 2, wherein the device is arranged to carry out a batch of on-line authentications of received certificates held in the store of received documents.

4. A device according to Claim 1, wherein each entry in the audit log contains a digest of the received document to which it relates.

5. A device according to Claim 4, further comprising a hash algorithm for creating a digest of a digital document and a receiving module for receiving a digital representation of a previously printed out document, wherein the device is arranged to create a digest of the digital representation of the previously printed out document and to compare the newly created digest with the corresponding digest stored in the audit log.

6. A device according to Claim 5, wherein the device is arranged to send either a stored digest or a newly created digest of a document to its original sender and to verify the authenticity of the document back to its source by considering the transmitted results of a comparison of digests carried out at the source.

7. A device according to Claim 5, wherein the receiving module is a document scanning module.

8. A device according to Claim 1, wherein each entry in the audit log contains the time and date of receipt of each digital document.

9. A device according to Claim 1, wherein the unique identifier is an alphanumeric code and the device further comprises an input module for inputting the code to access the relevant entry in the audit log.

10. In a facsimile machine adapted for receiving and printing out digital documents, a device comprising:

a store of digital certificates, each certificate being associated with a most recent sender of a received digital document; and

an audit log comprising a list of received document entries, each entry containing a reference to one of the certificates in the store and a unique identifier associated with a received digital document, wherein:

the received digital document and a digital certificate of a most recent sender of the received digital document are received contemporaneously by the facsimile machine; and

the facsimile machine is configured to print the received digital document upon the most recent sender of the received digital document being authenticated.

11. A method of authenticating the identity of a sender of a received digital document, the method comprising:

using a unique identifier printed on the received document to search for a corresponding record in a list of received document records;

referencing a digital certificate associated with the selected record, the certificate being one of a store of certificates of received documents and each digital certificate being associated with a most recent sender of a received digital document;

receiving an encrypted digest of the received digital document;

decrypting the encrypted digest;

computing a value of a second digest from the received digital document;

comparing the computed value of the second digest with a value of the decrypted digest;

carrying out an on-line authentication of the certificate when the computed value of the second digest corresponds with the value of the decrypted digest; and

printing the received digital document if the certificate of the most recent sender of the received digital document is authenticated, wherein the received digital document, the received encrypted digest associated with the received digital document, and the digital certificate associated with the received digital document are received contemporaneously.

12. A device according to Claim 1, wherein each digital certificate comprises a public key associated with a sender of the received digital document; wherein the decryption algorithm decrypts the encrypted digest using the sender's public key extracted from the digital certificate; wherein the hash algorithm computes a digest of a document copy, and wherein authenticity of the copied document is verified when the computed digest corresponds to the decrypted digest.

13. A device according to Claim 12, further comprising a remote device that encrypts the digest of the received digital document using the sender's private key.

14. A method according to Claim 11, wherein the digital certificate comprises a public key associated with the sender of the received digital document and wherein the encrypted digest is encrypted with a private key of the sender, the method further comprising:

decrypting the encrypted digest using the public key of the sender extracted from the certificate.

15. A method according to Claim 11, further comprising:

receiving a copy of a document;

computing a digest of the document copy;

comparing the computed digest with the decrypted digest; and

determining that the document copy is authentic when the computed digest corresponds to the decrypted digest.

16. A method according to Claim 11, wherein computing the digest of the document copy further comprises using a hash algorithm to compute the digest of the document copy, wherein the hash algorithm is the same as an original hash algorithm used to originally generate the decrypted digest.

Evidence Appendix under 37 C.F.R. § 41.37(c)(1)(ix)

There is no extrinsic evidence to be considered in this Appeal. Therefore, no evidence is presented in this Appendix.

Related Proceedings Appendix under 37 C.F.R. § 41.37(c)(1)(x)

There are no related proceedings to be considered in this Appeal. Therefore, no such proceedings are identified in this Appendix.

RECEIVED
CENTRAL FAX CENTER

SEP 1 3 2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 30006788-2

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Keith A. Harrison, et al.

Confirmation No.: 4475

Application No.: 09/918,326

Examiner: Schubert, Kevin R.

Filing Date: July 30, 2001

Group Art Unit: 2137

Title: Authentication Method in a Printing Environment

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on June 13, 2006.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $120	☐ 2nd Month $450	☐ 3rd Month $1020	☐ 4th Month $1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 500 . At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

☐ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit:

OR

☒ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.
Date of facsimile: September 13, 2006
Typed Name: Lindsey Corbin
Signature:

Respectfully submitted,
Keith A. Harrison, et al.
By
Charles W. Griggers
Attorney/Agent for Applicant(s)
Reg No. : 47,283
Date : September 13, 2006
Telephone : 770-933-9500

Rev 10/05 (AplBrief)